AN4108
Application note

How to set up a HTTPS server for In-Home display with HTTPS

Introduction

This application note describes how to configure a simple SSL web server using the EasyPHP free application to use the “In-Home display with HTTPS gateway” system.

The system is formed by an ST demonstration board connected to a network, and is capable of publishing the home automation devices (i.e. smartplugs) energy data to a remote web server. The user can consult the energy consumption data on the web server from wherever they are. From their home, they can manage the entire system by means of a touch panel.

The connection between the STM3221G-EVAL board and the web server is protected using SSL secure protocol. The SSL handshake process is based on RSA encryption (used for key exchange/signature implemented with a random number generator provided in the STM32 MCU), while the messages, exchanged between the STM3221G-EVAL board and the web server, are encrypted/decrypted using AES256.

- *Section 1* describes the document and library rules.
- *Section 2* shows the EasyPHP installation setup.
- *Section 3* explains how to get started with an Apache web server and how to configure a MySQL database suitable for the In-Home display with HTTPS gateway system.
- *Section 4* illustrates how to set up an Apache web server and configure a MySQL database to receive and store the energy consumption data report coming from the STM3221G-EVAL board running the In-Home display with HTTPS gateway firmware.

Contents

1 Document and library rules 4
1.1 Acronyms 4
2 EasyPHP installation setup 5
3 Set up Apache web server and configure a MySQL database 8
3.1 Apache configuration 8
3.2 Database structure definition and configuration 11
4 References 15
5 Revision history 16

List of figures

Figure 1. Select EasyPHP language . . . 5
Figure 2. EasyPHP set-up welcome screen . . . 5
Figure 3. EasyPHP license agreement . . . 6
Figure 4. EasyPHP information collected . . . 6
Figure 5. EasyPHP installation directory . . . 6
Figure 6. EasyPHP start menu shortcut name . . . 7
Figure 7. EasyPHP installation ready . . . 7
Figure 8. Apache configuration file "httpd.conf" . . . 8
Figure 9. Apache configuration step 1 . . . 9
Figure 10. Apache configuration step 2 . . . 9
Figure 11. Apache configuration step 3 . . . 10
Figure 12. Apache configuration step 4 . . . 10
Figure 13. Apache configuration step 5 . . . 11
Figure 14. EasyPHP administration access . . . 11
Figure 15. EasyPHP administration page . . . 12
Figure 16. Managing MySQL server . . . 12
Figure 17. Importing database scheme . . . 13
Figure 18. Selecting database scheme file . . . 13

1 Document and library rules

This document uses the conventions described below.

1.1 Acronyms

Table 1 lists the acronyms used in this document.

Table 1. List of acronyms

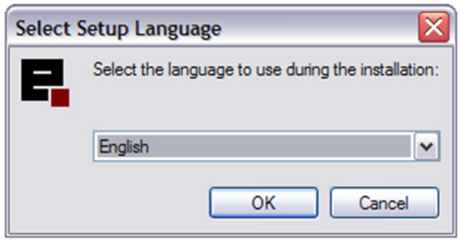
Acronym	Meaning
SSL	Secure socket layer
HTTPS	HyperText transfer protocol over secure socket layer

2 EasyPHP installation setup

For this reference design, EasyPHP 5.3.2i has been used. This release supports HTTPS protocol through SSL connection and the MySQL database engine.

First of all, download EasyPHP 5.3.2i, and then double click to start the installation, as shown in the following screen:

Figure 1. Select EasyPHP language



AM12289v1

Choose the installation language and click “OK”;

Figure 2. EasyPHP setup welcome screen

Setup - EasyPHP
Welcome to the EasyPHP Setup Wizard
This will install EasyPHP 5.2.10 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
About...
Next >
Cancel

AM12290v1

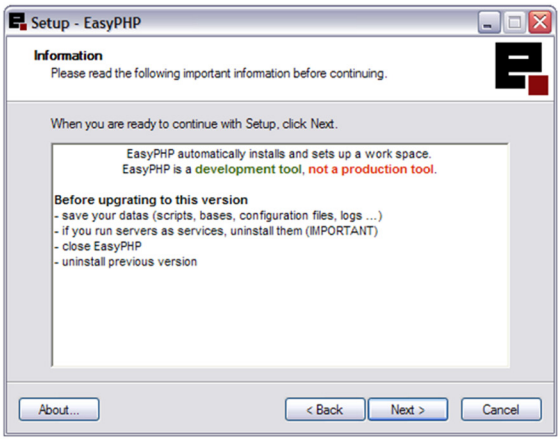
Click “Next” on this screen;

Figure 3. EasyPHP license agreement

AM12291v1

Select the option “I accept the agreement” and click “Next”;

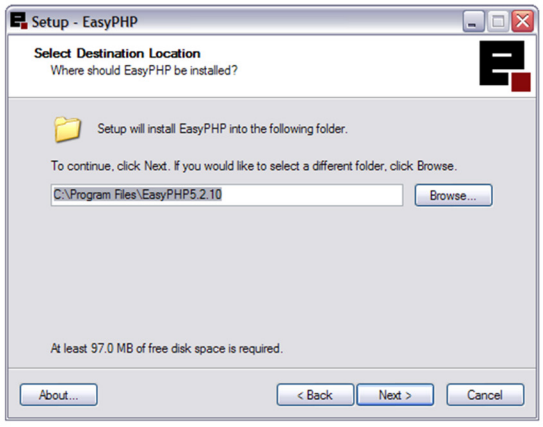
Figure 4. EasyPHP information collected



AM12292v1

Click “Next” again on this screen;

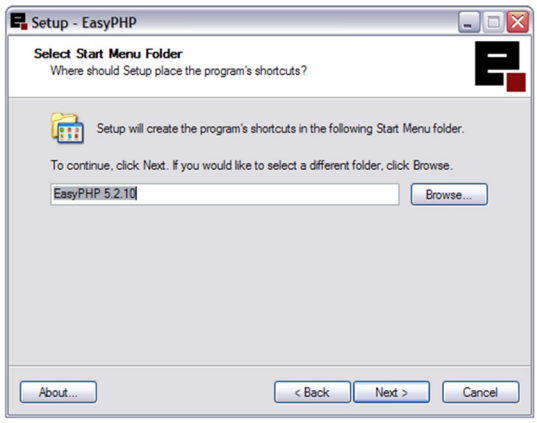
Figure 5. EasyPHP installation directory



AM12293v1

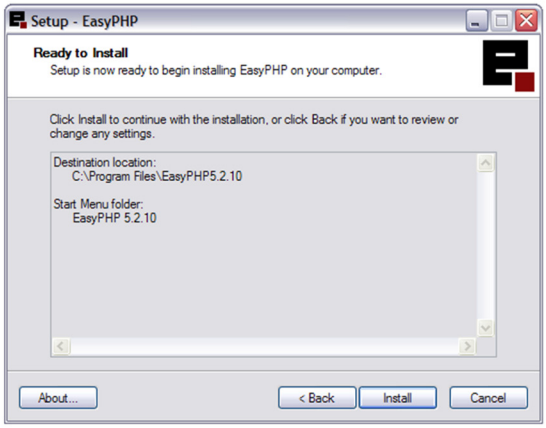
Choose the installation directory and click “Next”;

Figure 6. EasyPHP start menu shortcut name


Setup - EasyPHP
Select Start Menu Folder
Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
EasyPHP 5.2.10
Browse...
About...
< Back
Next >
Cancel
AM12294v1

Choose the name of the program shortcut on the Start Menu folder and click “Next”;

Figure 7. EasyPHP installation ready



Finally click on “Install” to complete the installation.

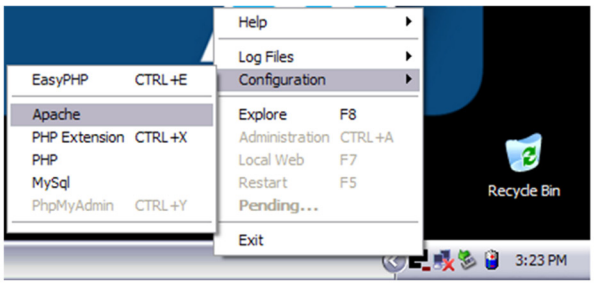
3 Set up Apache web server and configure a MySQL database

3.1 Apache configuration

When EasyPHP has been installed, go through the Apache configuration on the web server and the database structure.

Open Apache configuration file “httpd.conf” by right-clicking on the EasyPHP task icon, as shown below:

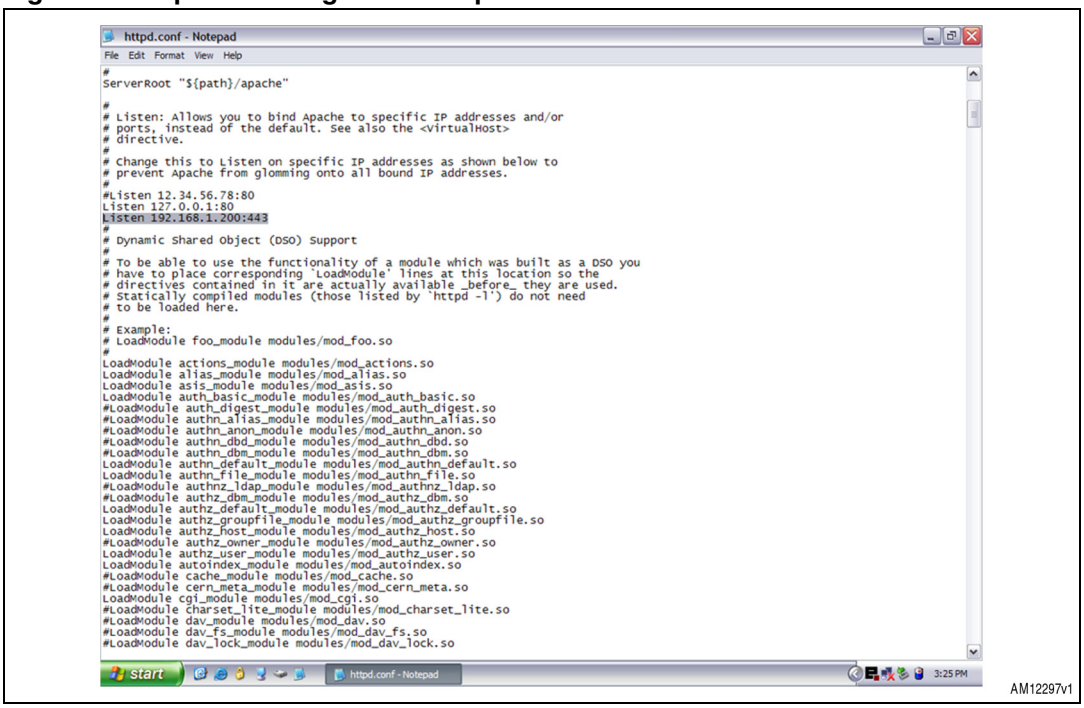
Figure 8. Apache configuration file “httpd.conf”



Follow the next screens in order to configure the Apache web server required for the company IT infrastructure or home network router configuration.

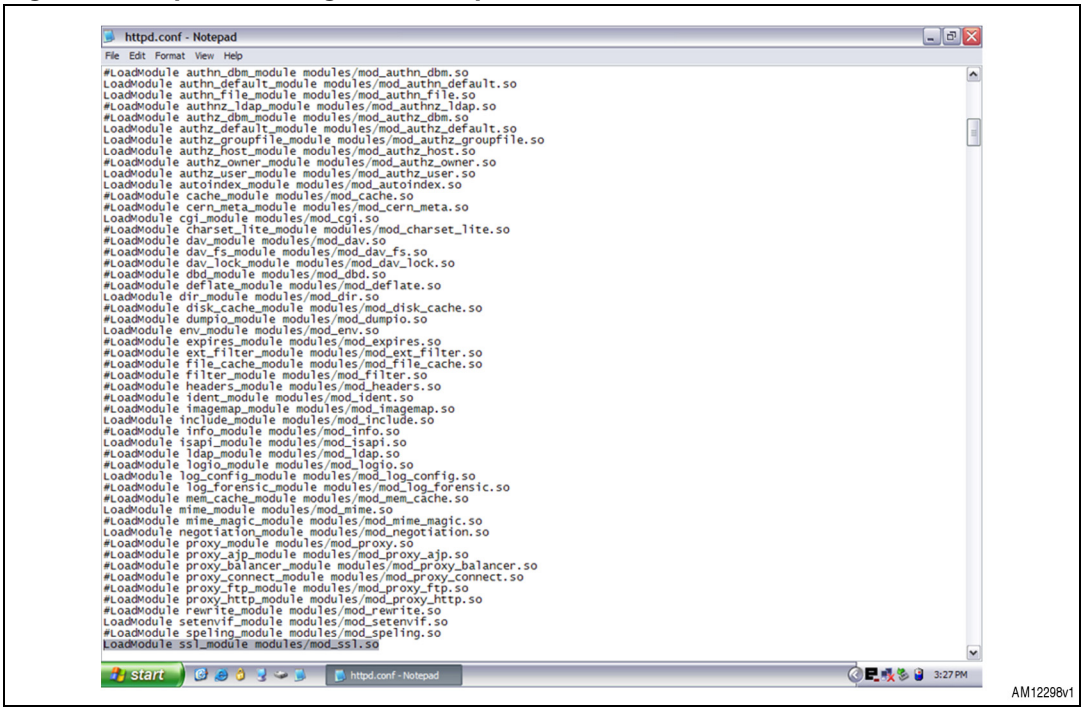
Locate the corresponding row on the following screen. It is necessary to indicate the IP address of the web server.

Figure 9. Apache configuration step 1


httpd.conf - Notepad
File Edit Format View Help
#
ServerRoot "${path}/apache"
#
Listen: Allows you to bind Apache to specific IP addresses and/or
ports, instead of the default. See also the <VirtualHost>
directive.
#
Change this to Listen on specific IP addresses as shown below to
prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 127.0.0.1:80
Listen 192.168.1.200:443
#
Dynamic Shared Object (DSO) Support
#
To be able to use the functionality of a module which was built as a DSO you
have to place corresponding `LoadModule' lines at this location so the
directives contained in it are actually available _before_ they are used.
Statically compiled modules (those listed by `httpd -l') do not need
to be loaded here.
#
Example:
LoadModule foo_module modules/mod_foo.so
#
LoadModule actions_module modules/mod_actions.so
LoadModule alias_module modules/mod_alias.so
LoadModule asis_module modules/mod_asis.so
LoadModule auth_basic_module modules/mod_auth_basic.so
#LoadModule auth_digest_module modules/mod_auth_digest.so
#LoadModule authn_alias_module modules/mod_authn_alias.so
#LoadModule authn_anon_module modules/mod_authn_anon.so
#LoadModule authn_dbd_module modules/mod_authn_dbd.so
#LoadModule authn_dbm_module modules/mod_authn_dbm.so
LoadModule authn_default_module modules/mod_authn_default.so
LoadModule authn_file_module modules/mod_authn_file.so
#LoadModule authnz_ldap_module modules/mod_authnz_ldap.so
#LoadModule authz_dbm_module modules/mod_authz_dbm.so
LoadModule authz_default_module modules/mod_authz_default.so
LoadModule authz_groupfile_module modules/mod_authz_groupfile.so
LoadModule authz_host_module modules/mod_authz_host.so
#LoadModule authz_owner_module modules/mod_authz_owner.so
LoadModule authz_user_module modules/mod_authz_user.so
LoadModule autoindex_module modules/mod_autoindex.so
#LoadModule cache_module modules/mod_cache.so
#LoadModule cern_meta_module modules/mod_cern_meta.so
LoadModule cgi_module modules/mod_cgi.so
#LoadModule charset_lite_module modules/mod_charset_lite.so
#LoadModule dav_module modules/mod_dav.so
#LoadModule dav_fs_module modules/mod_dav_fs.so
#LoadModule dav_lock_module modules/mod_dav_lock.so
start
httpd.conf - Notepad
3:25 PM
AM12297v1

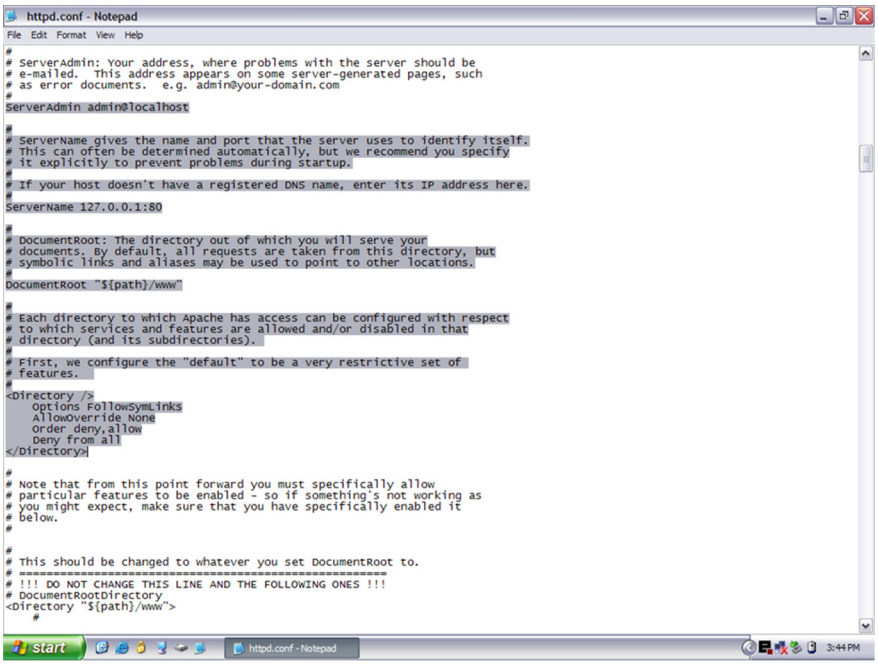
Then, look at the following screen and locate the corresponding row. Here it is necessary to delete the comment symbol “#” in order to enable the SSL module.

Figure 10. Apache configuration step 2



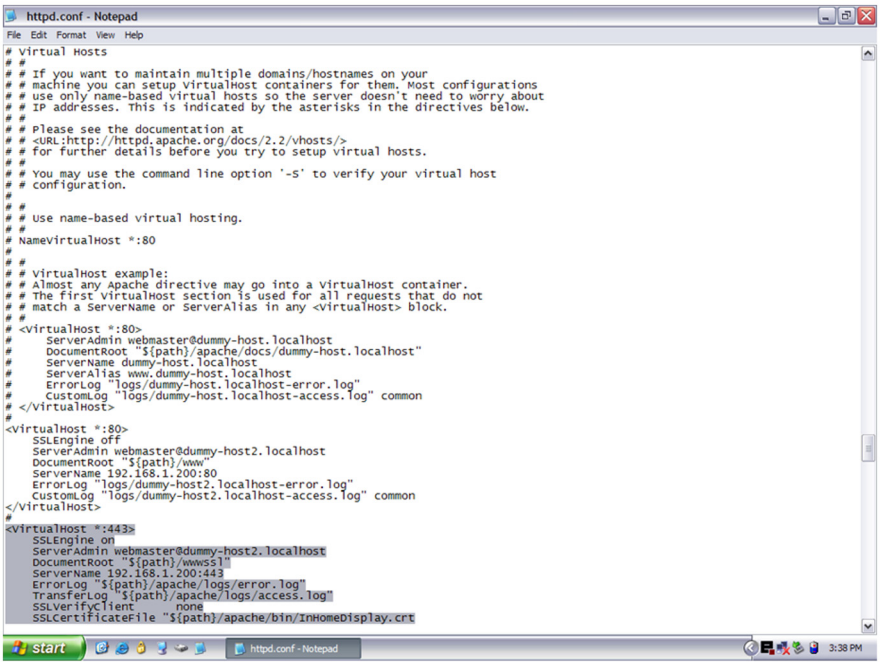
Now, locate the corresponding row on the following screen. This section aims to configure the server parameters such as e-mail address, server name, listening port, and document root (where the website is published and the respective access permission).

Figure 11. Apache configuration step 3


httpd.conf - Notepad
File Edit Format View Help
ServerAdmin: Your address, where problems with the server should be
e-mailed. This address appears on some server-generated pages, such
as error documents. e.g. admin@your-domain.com
ServerAdmin admin@localhost
ServerName gives the name and port that the server uses to identify itself.
This can often be determined automatically, but we recommend you specify
it explicitly to prevent problems during startup.
If your host doesn't have a registered DNS name, enter its IP address here.
ServerName 127.0.0.1:80
DocumentRoot: The directory out of which you will serve your
documents. By default, all requests are taken from this directory, but
symbolic links and aliases may be used to point to other locations.
DocumentRoot "${path}/www"
Each directory to which Apache has access can be configured with respect
to which services and features are allowed and/or disabled in that
directory (and its subdirectories).
First, we configure the "default" to be a very restrictive set of
features.
<Directory />
Options FollowSymLinks
AllowOverride None
Order deny,allow
Deny from all
</Directory>
Note that from this point forward you must specifically allow
particular features to be enabled - so if something's not working as
you might expect, make sure that you have specifically enabled it
below.
This should be changed to whatever you set DocumentRoot to.
!!! DO NOT CHANGE THIS LINE AND THE FOLLOWING ONES !!!
DocumentRootDirectory
<Directory "${path}/www">
start
httpd.conf - Notepad
3:44 PM
AM12299v1

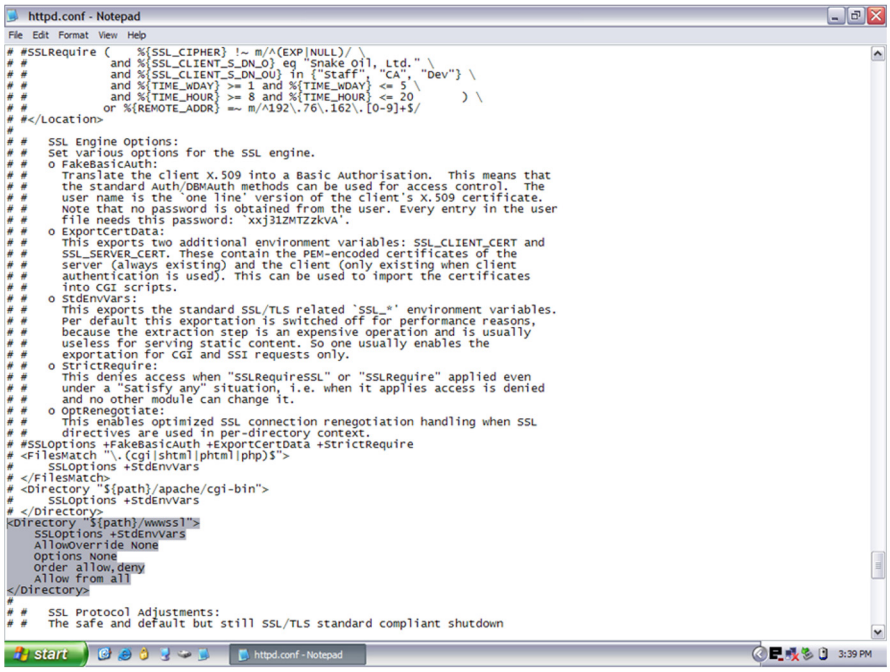
After that, it is possible to see, on the following screen, the highlighted code with respect to the web server and the website directory configuration.

Figure 12. Apache configuration step 4


httpd.conf - Notepad
File Edit Format View Help
Virtual Hosts
If you want to maintain multiple domains/hostnames on your
machine you can setup VirtualHost containers for them. Most configurations
use only name-based virtual hosts so the server doesn't need to worry about
IP addresses. This is indicated by the asterisks in the directives below.
Please see the documentation at
<URL:http://httpd.apache.org/docs/2.2/vhosts/>
for further details before you try to setup virtual hosts.
You may use the command line option '-S' to verify your virtual host
configuration.
Use name-based virtual hosting.
NameVirtualHost *:80
VirtualHost example:
Almost any Apache directive may go into a VirtualHost container.
The first VirtualHost section is used for all requests that do not
match a ServerName or ServerAlias in any <VirtualHost> block.
<VirtualHost *:80>
ServerAdmin webmaster@dummy-host.localhost
DocumentRoot "${path}/apache/docs/dummy-host.localhost"
ServerName dummy-host.localhost
ServerAlias www.dummy-host.localhost
ErrorLog "logs/dummy-host.localhost-error.log"
CustomLog "logs/dummy-host.localhost-access.log" common
</VirtualHost>
<VirtualHost *:80>
SSLEngine off
ServerAdmin webmaster@dummy-host2.localhost
DocumentRoot "${path}/www"
ServerName 192.168.1.200:80
ErrorLog "logs/dummy-host2.localhost-error.log"
CustomLog "logs/dummy-host2.localhost-access.log" common
</VirtualHost>
<VirtualHost *:443>
SSLEngine on
ServerAdmin webmaster@dummy-host2.localhost
DocumentRoot "${path}/wwwssl"
ServerName 192.168.1.200:443
ErrorLog "${path}/apache/logs/error.log"
TransferLog "${path}/apache/logs/access.log"
SSLVerifyClient none
SSLCertificateFile "${path}/apache/bin/InHomeDisplay.crt
start
httpd.conf - Notepad
3:38 PM
AM12300v1

Finally, look at the following screen and the highlighted code with respect to the website directory configuration in order to set the folder permission.

Figure 13. Apache configuration step 5


httpd.conf - Notepad
File Edit Format View Help
#SSLRequire (%{SSL_CIPHER} !~ m/^(EXP|NULL)/ \
and %{SSL_CLIENT_S_DN_O} eq "Snake Oil, Ltd." \
and %{SSL_CLIENT_S_DN_OU} in {"Staff", "CA", "Dev"} \
and %{TIME_WDAY} >= 1 and %{TIME_WDAY} <= 5 \
and %{TIME_HOUR} >= 8 and %{TIME_HOUR} <= 20) \
or %{REMOTE_ADDR} =~ m/^192\.76\.162\.[0-9]+$/
#</Location>
SSL Engine Options:
Set various options for the SSL engine.
o FakeBasicAuth:
Translate the client X.509 into a Basic Authorisation. This means that
the standard Auth/DBMAuth methods can be used for access control. The
user name is the `one line' version of the client's X.509 certificate.
Note that no password is obtained from the user. Every entry in the user
file needs this password: `xxj31ZMTZzkVA'.
o ExportCertData:
This exports two additional environment variables: SSL_CLIENT_CERT and
SSL_SERVER_CERT. These contain the PEM-encoded certificates of the
server (always existing) and the client (only existing when client
authentication is used). This can be used to import the certificates
into CGI scripts.
o StdEnvVars:
This exports the standard SSL/TLS related `SSL_*' environment variables.
Per default this exportation is switched off for performance reasons,
because the extraction step is an expensive operation and is usually
useless for serving static content. So one usually enables the
exportation for CGI and SSI requests only.
o StrictRequire:
This denies access when "SSLRequireSSL" or "SSLRequire" applied even
under a "Satisfy any" situation, i.e. when it applies access is denied
and no other module can change it.
o OptRenegotiate:
This enables optimized SSL connection renegotiation handling when SSL
directives are used in per-directory context.
#SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
<FilesMatch "\.(cgi|shtml|phtml|php)$">
SSLOptions +StdEnvVars
</FilesMatch>
<Directory "${path}/apache/cgi-bin">
SSLOptions +StdEnvVars
</Directory>
<Directory "${path}/wwwssl">
SSLOptions +StdEnvVars
AllowOverride None
Options None
Order allow,deny
Allow from all
</Directory>
#
SSL Protocol Adjustments:
The safe and default but still SSL/TLS standard compliant shutdown
start
httpd.conf - Notepad
3:39 PM
AM12301v1

3.2 Database structure definition and configuration

Each time a smartplug node joins the network and its load type is configured through the GUI interface, it starts reporting power and energy consumption measured values.

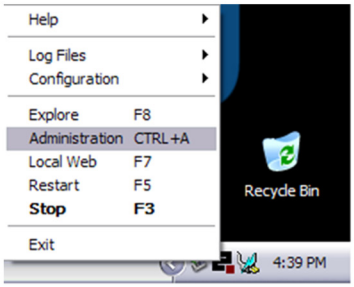
This data is received from the coordinator board and routed via Ethernet to the web server using SSL connection.

The user can browse this data from another PC connecting to the web server and logging in with a username and password. Then, the user can view the reporting table, export data to an Excel file, or plot it to graphical charts.

In order to permit all these functions, it is necessary to properly configure a database on the web server using the MySQL database engine embedded in EasyPHP. For simplicity, an SQL file containing the database schema is available in the In-Home display with HTTPS gateway set-up package, and so it just needs to be imported.

Open the EasyPHP administration page, as shown on the following screen:

Figure 14. EasyPHP administration access



On the following screen click on “Manage MySQL”:

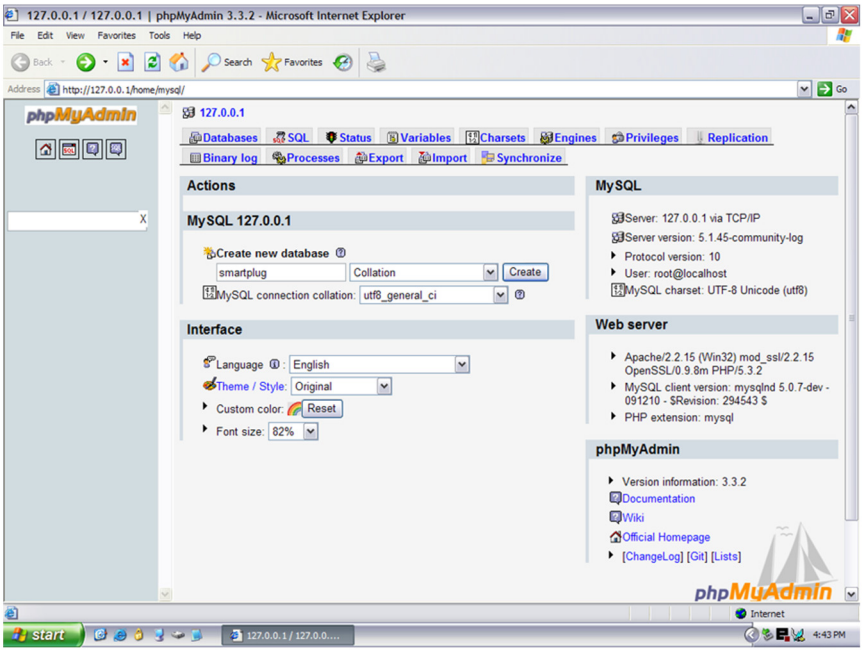
Figure 15. EasyPHP administration page

[EasyPHP] - Administration - Microsoft Internet Explorer
www.easyphp.org
Support, download, faq, news, forum...
PHP 5.3 migration guide
Most improvements in PHP 5.3.x have no impact on existing code.
However, there are a few incompatibilities and new features that should be considered.
If you want to use EasyPHP on an USB key, you just need to copy the entire EasyPHP folder on the key. Be sure that all your scripts are in the folder 'www' and your databases in 'mysql\data'.
PHP 5.3.2
APACHE 2.2.15
MYSQL 5.1.45
PHPMYADMIN 3.3.2
Manage MySQL
MySQL Parameters
PHP Parameters
Time Zone
Extensions
LOCAL WEB
C:\Program Files\EasyPHP-5.3.2\www\
Root
images
jpgraph
"ALIAS"
add
MODULES
download
start
4:41 PM

AM12303v1

Then, the following screen is shown:

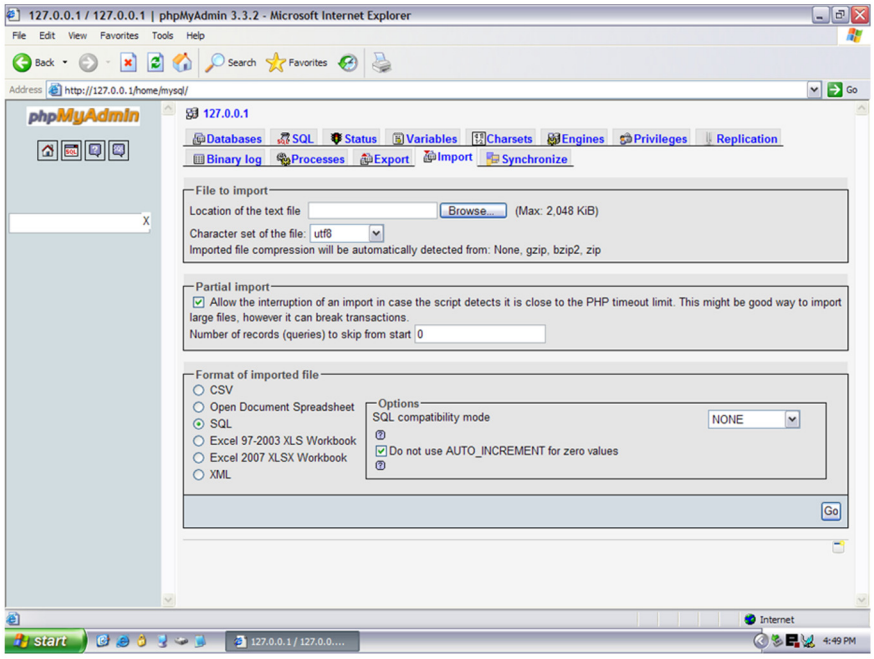
Figure 16. Managing MySQL server



AM12304v1

From this screen, first create a new database called “smartplug” by clicking on “Create”. Then, click on the “Import” tab in order to visualize the following screen from which it is possible to import the database schema file.

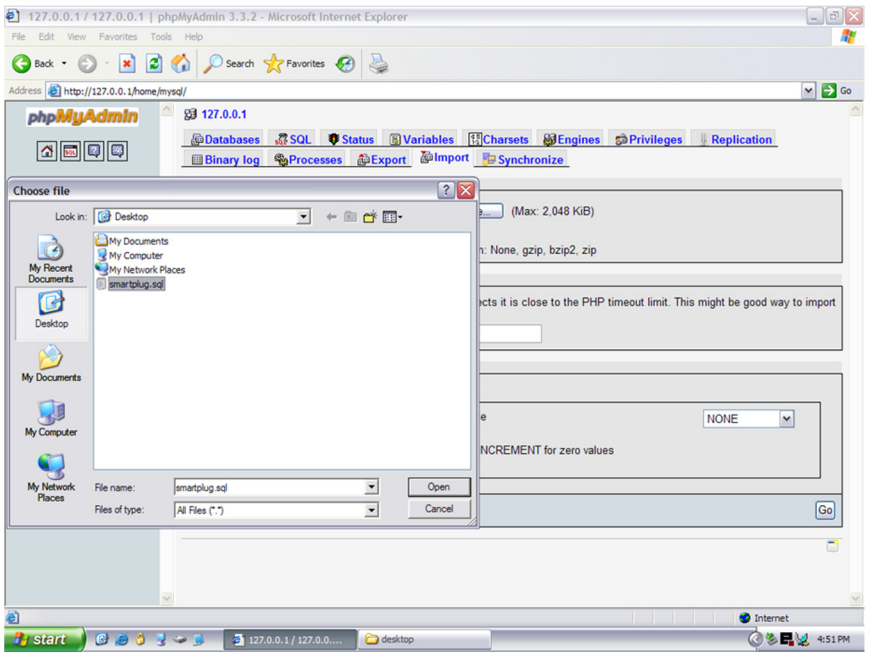
Figure 17. Importing database scheme


127.0.0.1 / 127.0.0.1 | phpMyAdmin 3.3.2 - Microsoft Internet Explorer
phpMyAdmin
127.0.0.1
Databases SQL Status Variables Charsets Engines Privileges Replication
Binary log Processes Export Import Synchronize
File to import
Location of the text file
Browse...
(Max: 2,048 KiB)
Character set of the file: utf8
Imported file compression will be automatically detected from: None, gzip, bzip2, zip
Partial import
Allow the interruption of an import in case the script detects it is close to the PHP timeout limit. This might be good way to import large files, however it can break transactions.
Number of records (queries) to skip from start 0
Format of imported file
CSV
Open Document Spreadsheet
SQL
Excel 97-2003 XLS Workbook
Excel 2007 XLSX Workbook
XML
Options
SQL compatibility mode
NONE
Do not use AUTO_INCREMENT for zero values
Go
start
4:49 PM

AM12305v1

Click on “Browse” and select the database schema file, as shown on the following screen:

Figure 18. Selecting database scheme file



AM12306v1

Finally, click on “Go” to import the database structure.

At this stage both the Apache web server and MySQL database have been configured. So, the system is ready to receive and store data coming from the STM3221G-EVAL running the In-Home display with HTTPS gateway firmware.

4 References

1. AN4049 - application note
2. UM1065 - user manual
3. AN3365_Rev1 - application note
4. UM1519 - user manual

5 Revision history

Table 2. Document revision history

Date	Revision	Changes
25-Sep-2012	1	Initial release.

Please Read Carefully:

Information in this document is provided solely in connection with ST products. STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, modifications or improvements, to this document, and the products and services described herein at any time, without notice.

All ST products are sold pursuant to ST’s terms and conditions of sale.

Purchasers are solely responsible for the choice, selection and use of the ST products and services described herein, and ST assumes no liability whatsoever relating to the choice, selection or use of the ST products and services described herein.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted under this document. If any part of this document refers to any third party products or services it shall not be deemed a license grant by ST for the use of such third party products or services, or any intellectual property contained therein or considered as a warranty covering the use in any manner whatsoever of such third party products or services or any intellectual property contained therein.

UNLESS OTHERWISE SET FORTH IN ST’S TERMS AND CONDITIONS OF SALE ST DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE USE AND/OR SALE OF ST PRODUCTS INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE (AND THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION), OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS EXPRESSLY APPROVED IN WRITING BY TWO AUTHORIZED ST REPRESENTATIVES, ST PRODUCTS ARE NOT RECOMMENDED, AUTHORIZED OR WARRANTED FOR USE IN MILITARY, AIR CRAFT, SPACE, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS, NOR IN PRODUCTS OR SYSTEMS WHERE FAILURE OR MALFUNCTION MAY RESULT IN PERSONAL INJURY, DEATH, OR SEVERE PROPERTY OR ENVIRONMENTAL DAMAGE. ST PRODUCTS WHICH ARE NOT SPECIFIED AS "AUTOMOTIVE GRADE" MAY ONLY BE USED IN AUTOMOTIVE APPLICATIONS AT USER’S OWN RISK.

Resale of ST products with provisions different from the statements and/or technical features set forth in this document shall immediately void any warranty granted by ST for the ST product or service described herein and shall not create or extend in any manner whatsoever, any liability of ST.

ST and the ST logo are trademarks or registered trademarks of ST in various countries.

Information in this document supersedes and replaces all information previously supplied.

The ST logo is a registered trademark of STMicroelectronics. All other names are the property of their respective owners.

© 2012 STMicroelectronics - All rights reserved

STMicroelectronics group of companies

Australia - Belgium - Brazil - Canada - China - Czech Republic - Finland - France - Germany - Hong Kong - India - Israel - Italy - Japan - Malaysia - Malta - Morocco - Philippines - Singapore - Spain - Sweden - Switzerland - United Kingdom - United States of America

www.st.com